IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

MICHAEL W. TILLEMAN, individually and on behalf of all others similarly situated, Plaintiff, v. LEAFFILTER NORTH, LLC; and LEAFFILTER NORTH OF TEXAS, LLC, Defendants.	Case No. 5:18-cv-1152

CLASS ACTION COMPLAINT

William B. Federman (Bar No. 00794935)
FEDERMAN & SHERWOOD
2926 Maple Ave., Ste. 200
Dallas, TX 75201
Telephone: (214) 696-1100
Facsimile: (214) 740-0112
wbf@federmanlaw.com

ATTORNEY FOR PLAINTIFF AND
THE PROPOSED CLASS

November 2, 2018

TABLE OF CONTENTS

COMES NOW Plaintiff Michael W. Tilleman, individually ("Plaintiff') and on behalf of all others similarly situated (*i.e.* the members of the Class described and defined within this Class Action Complaint) (the "Class"), and for his causes of action against Defendants LeafFilter North, LLC and LeafFilter North of Texas, LLC ("Defendants" or "LeafFilter"), alleges and states as follows:

I. THE PARTIES

1. Plaintiff Michael W. Tilleman is a citizen of the State of Texas and a resident of Bexar County, Texas.

2. Defendant LeafFilter North, LLC is an Ohio limited liability company doing business as "LeafFilter North" that is organized under the laws of the State of Ohio and whose headquarters is located in Hudson, Ohio.

3. Defendant LeafFilter North of Texas, LLC is an Ohio limited liability company doing business as "LeafFilter North" that is organized under the laws of the State of Ohio and who maintains offices in Austin, Grand Prairie, and Houston, Texas.

4. Defendants manufacture, market, sell, and install a guttering system for residential and commercial buildings that, they claim, permits water but not leaves and debris to flow through, thereby preventing clogged gutters and resulting structural damage.

5. Defendants maintain more than fifty offices throughout the United States and Canada, including at least one office in this District.

II. JURISDICTION AND VENUE

6. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

7. This Court has diversity jurisdiction over this action under 28 U.S.C. § 1332(a) because Plaintiff is a citizen of a different state than Defendants and the amount in controversy exceeds $75,000, exclusive of interest and costs.

8. This Court has diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action in which Plaintiff and the Class are citizens of a different state than Defendants and the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

9. This Court has personal jurisdiction over Plaintiff because he resides in Bexar County, Texas, which is within the Court's jurisdiction.

10. This Court has personal jurisdiction over Defendants because Defendants have conducted and continue to conduct substantial business in this State and because Defendants have committed the acts and omissions complained of herein in this State.

11. Venue as to Defendants is proper in this judicial district under 28 U.S.C § 1391(b)(1) because Defendants maintain a business office in this District, advertise and engage in business in this District, employ persons who reside in this District and many of Defendants' acts complained of herein occurred within this District.

III. FACTUAL ALLEGATIONS

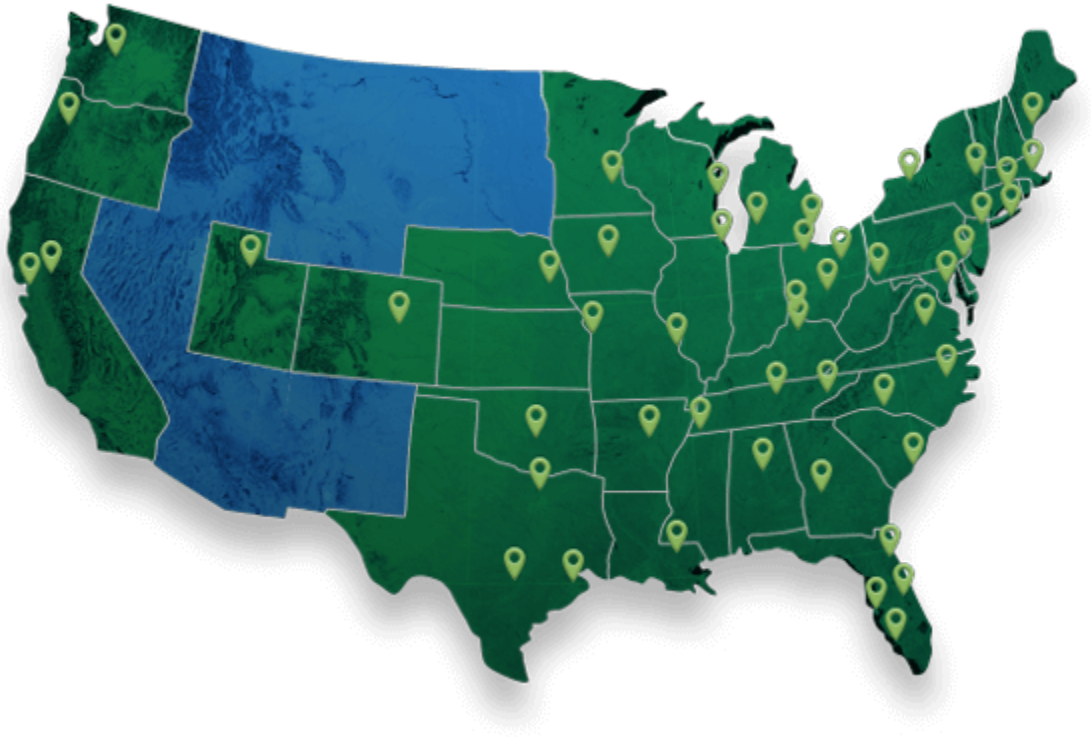
12. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

13. On its webpage, LeafFilter claims to be "The Nation's Largest Gutter Protection Company" and to have 223,260 customers. https://www.leaffilter.com/ (last visited Oct. 25, 2018).

14. LeafFilter sells and installs its gutter protection system "[f]rom coast to coast." Source: https://www.leaffilter.com/ (last visited Oct. 25, 2018).

15. LeafFilter recently opened its 52nd office. Source: https://www.leaffilter.com/press/leaffilter-opens-orlando-office/ (last visited Oct. 25, 2018).

16. LeafFilter has employees and subcontractors in forty (40) states engaged in the manufacture, marketing, sale, and installation of its gutter protection system:



Source: https://www.leaffilter.com/ (last visited Oct. 25, 2018).

17. In 2018, Plaintiff applied for a job with Defendants at their business office in Austin, Texas.

18. Defendants offered Plaintiff the job and requested that he provide them with certain personal identifying information ("PII").

19. Plaintiff provided Defendants with his PII, including his (a) driver's license, which contained Plaintiff's name, address, date of birth, and driver's license number; (b) social security number; and (c) bank account information.

20. The information that Plaintiff provided to Defendants falls with the definition of "personal identifying information" under the Texas statutes, which provide that "'[p]ersonal identifying information' means information that alone or in conjunction with other information identifies an individual, including an individual's:

(A) name, social security number, date of birth, or government-issued identification number;
(B) mother's maiden name;
(C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
(D) unique electronic identification number, address, or routing code; and
(E) telecommunication access device as defined by Section 32.51, Penal Code.

TEX. BUS. & COMM. CODE § 521.002(a)(1).

21. Alternatively, the information that Plaintiff provided to Defendants falls with the definition of "sensitive personal information" under the Texas statutes, which provide that "'[s]ensitive personal information' means, subject to Subsection (b):

(A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
    (i) social security number;
    (ii) driver's license number or government-issued identification number; or
    (iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
(B) information that identifies an individual and relates to:
    (i) the physical or mental health or condition of the individual;
    (ii) the provision of health care to the individual; or
    (iii) payment for the provision of health care to the individual.

TEX. BUS. & COMM. CODE § 521.002(a)(2).

22. Plaintiff has a subscription with Credit Karma, a company that provides monitoring and alerts on his credit reports.

23. In August, 2018, Plaintiff received notice from Credit Karma of hard inquiry on his credit (*i.e.* that someone had applied for a credit account and the creditor pulled his credit report) by Wal-Mart/Synchrony Bank.

24. Plaintiff knew this activity was fraudulent because he had not applied for credit from Wal-Mart/Synchrony Bank and had not authorized them to pull his credit.

25. Plaintiff promptly contacted Wal-Mart/Synchrony Bank, notified them of the fraud, and requested that they close the account.

26. Plaintiff promptly contacted each of the credit bureaus to place a freeze on his credit so that no further credit could be taken out utilizing his PII without his specific authorization.

27. Plaintiff had to pay a fee to one of the credit bureaus for to lace a freeze on his credit.

28. Plaintiff has been and will continue to be inconvenienced by the credit freeze, which requires him to spend extra time unfreezing his account with each credit bureau any time he wants to make use of his own credit. By way of specific example, Plaintiff recently sought to take advantage of a retailer's offer of a discount for applying for and opening a store credit account. His application, however, was denied because of the credit freeze. Plaintiff then had to spend approximately one half an hour on the phone with the credit bureau to get it to temporarily unfreeze his account so the retailer could re-run his credit so he could obtain the credit account and discount.

29. Among other things, the age of accounts, the number of accounts, and the number of hard inquiries impacts a person's credit score. Source: *Confused about credit? So are a lot of people. Let's fix that.* by Mika Bhatia, Sept. 13, 2018, found at https://www.creditkarma.com/advice/i/learn-credit-score-factors/ (last visited Oct. 25, 2018).

30. Since the account with Wal-Mart/Synchrony Bank was opened and subsequently closed, Plaintiff's credit score decreased.

31. The decrease in Plaintiff's credit score may prohibit him from obtaining credit or make it more expensive for him to borrow funds in the future, cause him to have to pay a larger security deposit for utilities or a rental home, increase the cost of insurance, and/or negatively affect his ability to obtain a job. *See, e.g., What is Credit and How Is It Used?* by Justin Pritchard, Mar. 11, 2018, found at https://www.thebalance.com/what-is-credit-315391 (last visited Oct. 25, 2018). In fact, Plaintiff is in the market for a new car and has had to delay his purchase until his credit improves because the decrease in his credit score caused the cost of a loan from his financial institution to increase by three quarters of a percent (0.75%).

32. On or about October 8, 2018, Plaintiff received a letter in the mail from LeafFilter advising him of a "security incident" that Defendants discovered on or before August 21, 2018. *Letter from Larry Napolitan to Michael Tilleman*, dated October 4, 2018, Exhibit 1 hereto (hereafter, the "October 4 Letter"). According to the October 4 Letter, unauthorized persons used a phishing email to gain access to LeafFilter employees' email accounts which contained the personal information of Plaintiff and others. *Id.* (Hereafter, the events described in the October 4 Letter will be referred to as the "Data Breach").

33. After receiving the October 4 Letter, Plaintiff called the number provided in the October 4 Letter for more information. LeafFilter's Chief Financial Officer, Larry Napolitan, returned Plaintiff's call on or about October 10, 2018 and apologized for the Data Breach. Mr. Napolitan told Plaintiff that he was one of 3,000 people whose personal information had been compromised in the Data Breach.

34. Plaintiff has not been the victim of any other data breach in the last ten (10) years.

35. As reported by the FTC in 2017, if hackers get access to PII, they ***will*** use it. Source: *How fast will identity thieves use stolen info?* Ari Lazarus, May 24, 2017, found at https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info (last visited Oct. 26, 2018). The truth of these findings is borne out by Plaintiff's own experience, with his PII being used to commit identity theft (*i.e.* to fraudulently apply for and open a credit account using Plaintiffs' PII).

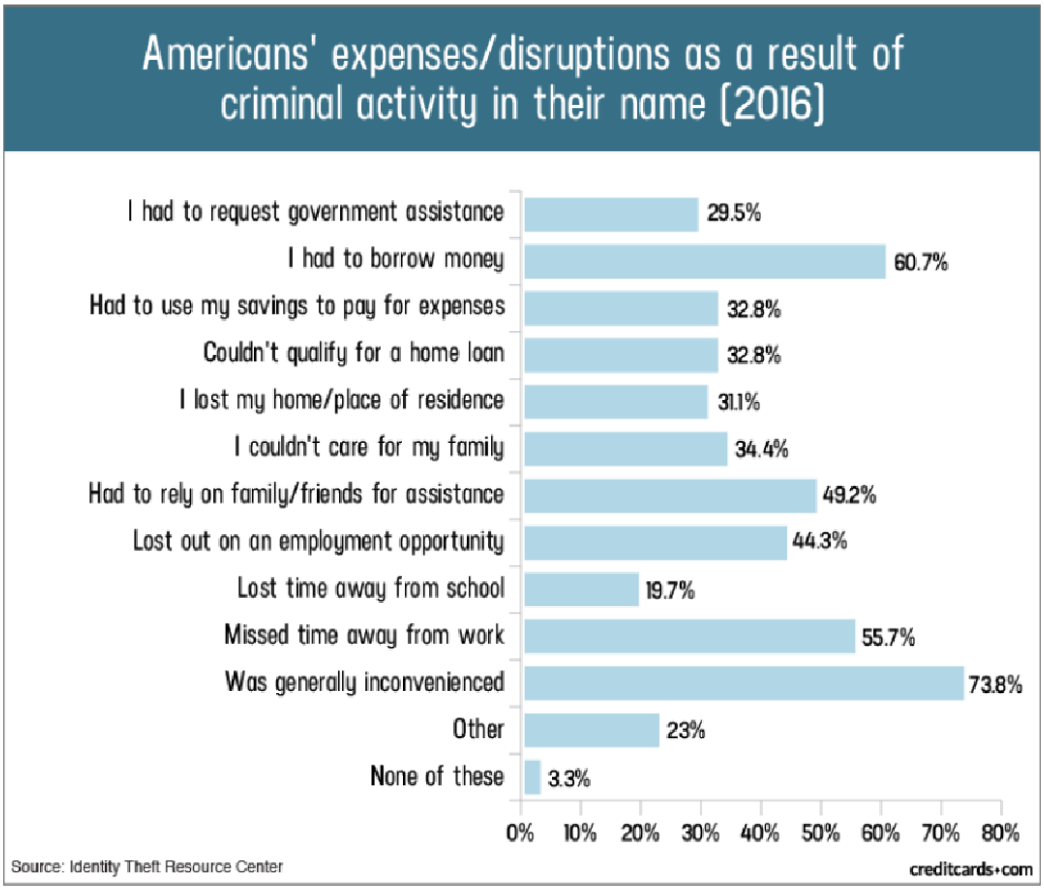
36. Hackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown by GAO, July 5, 2007, found at: https://www.gao.gov/assets/270/262904.htmlu (last visited Oct. 29, 2017).

37. With a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts (as has already happened to Plaintiff), get medical care, file fraudulent tax returns, commit crimes, and steal benefits. *See e.g., 5 Ways an Identity Thief Can Use Your Social Security Number* by Christine DiGangi, Nov. 2, 2017, found at https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Oct. 26, 2018).

38. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII such as that compromised in the Data Breach:



Source: "Credit Card and ID Theft Statistics" by Jason Steele, Oct. 24, 2017, found at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php. Plaintiff and the Class have experienced one or more of these harms as a result of the Data Breach.

39. Defendants' offer of one year of credit monitoring to Plaintiff and the Class is inadequate because it does not continue long enough. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. Furthermore, credit monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.* fraudulent acquisition and use of another person's PII) – it does not prevent identity theft. *See, e.g. Credit Monitoring Services May Not Be Worth the Cost* by

Kayleigh Kulp, Nov. 30, 2017, found at https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited Oct. 29, 2017).

40. As a direct and proximate result of the Data Breach, Plaintiff and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Class now have to take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

41. Plaintiff and the Class have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and having been already misused;

d. Damages flowing from Defendants untimely and inadequate notification of the data breach;

e. Loss of privacy suffered as a result of the data breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

g. Ascertainable losses in the form of deprivation of the value of customers' personal information for which there is a well-established and quantifiable national and international market;

h. The loss of use of and access to their credit, accounts, and/or funds;

i. Damage to their credit due to fraudulent use of their PII; and

j. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

42. Moreover, Plaintiff and the Class have an interest in ensuring that their information, which remains in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards.

IV. CLASS ALLEGATIONS

43. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

A. NATIONWIDE CLASS

44. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts common law claims for negligence (Count I), negligence per se (Count II), breach of implied contract (Count III), and injunctive / declaratory relief (Count IV), on behalf of a nationwide class, defined as follows:

All persons whose personal information was compromised by the Data Breach.

45. Excluded from the Class are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

B. STATEWIDE CLASSES

46. Alternatively, pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts common law claims for negligence (Count I), negligence per se (Count II), breach of implied contract (Count III), and injunctive / declaratory relief (Count IV), on behalf of separate statewide classes for each of the forty (40) states in which Defendants do business in which Plaintiff and/or members of the Class reside (Alabama, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Nebraska, New Hampshire, New Jersey, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin), defined as follows:

> **Statewide [name of State] Class: All residents of [name of State] whose personal information was compromised by the Data Breach.**

47. Excluded from the Class are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

C. CLASS CERTIFICATION IS APPROPRIATE

48. The proposed Nationwide Class or, alternatively, the separate Statewide Classes (collectively, the "Class" as used in this sub-section) meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

49. **Numerosity:** After Plaintiff received the October 4 Letter from LeafFilter, he called the company for more information. Larry Napolitan, LeafFilter's Chief Financial Officer

told Plaintiff, during a telephone conversation on or about October 10, 2018, that Plaintiff was one of approximately 3,000 people whose personal information was compromised in the Data Breach.

50. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendants failed to adequately safeguard Plaintiff's and the Class' PII;

b. Whether Defendants failed to protect Plaintiff's and the Class' PII;

c. Whether Defendants' email and computer systems and data security practices used to protect Plaintiff's and the Class' PII violated federal and/or state laws and/or Defendants' duties;

d. Whether Defendants violated the data security statutes and data breach notification statutes applicable to Plaintiff and the Class;

e. Whether Defendants failed to notify Plaintiff and members of the Class about the Data Breach expeditiously and without unreasonable delay after the Data Breach was discovered;

f. Whether Defendants acted negligently in failing to safeguard Plaintiff's and the Class' PII;

g. Whether Defendants entered into implied contracts with Plaintiff and the members of the Class that included contract terms requiring Defendants to protect the confidentiality of PII and have reasonable security measures;

h. Whether Defendants' conduct described herein constitutes a breach of their implied contracts with Plaintiff and the Class;

i. Whether Plaintiff and the members of the Class are entitled to damages as a result of Defendants' wrongful conduct;

j. What equitable relief is appropriate to redress Defendants' wrongful conduct; and

k. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by members of the Class.

51. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the members of the Class sustained damages as a result of Defendants' uniform wrongful conduct.

52. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

53. **Risks of Prosecuting Separate Actions:** This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendants or would be dispositive of the interests of members of the proposed Class. Furthermore, Defendants are still in possession of PII of Plaintiff and the Class, and Defendants' systems are still vulnerable to attack – one standard of conduct is needed to ensure the future safety of PII in Defendants' possession.

54. **Policies Generally Applicable to the Class:** This case is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to Plaintiff and the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendants' practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendants' conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

55. **Superiority:** This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendants' conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendants. Even if members of the Class could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

V. CAUSES OF ACTION

COUNT I – NEGLIGENCE
(Brought by the Nationwide Class or, alternatively, 40 Statewide Classes)

56. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

57. Defendants solicited, gathered, and stored the PII of Plaintiff and the Nationwide Negligence Class or, alternatively, the Separate Statewide Negligence Classes (collectively, the "Class" as used in this Count).

58. Defendants knew, or should have known, of the risks inherent in collecting and storing the PII of Plaintiff and the Class and the importance of adequate security.

59. Defendants were well aware of the fact that hackers routinely attempted to access PII without authorization. Defendants also knew about numerous, well-publicized data breaches wherein hackers stole the PII from companies who held or stored such information.

60. Defendants owed duties of care to Plaintiff and the Class whose PII was entrusted to it. Defendants' duties included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

b. To protect the PII in its possession using reasonable and adequate security procedures and systems;

c. To adequately and properly train its employees to avoid phishing emails;

d. To adequately and properly train its employees regarding how to properly and securely transmit and store PII;

e. To implement processes to quickly detect a data breach, security incident, or intrusion; and

f. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their PII.

61. Because Defendants knew that a security incident, breach or intrusion upon its systems would potentially damage thousands of its current, former or prospective employees and/or customers, including Plaintiff and Class members, it had a duty to adequately protect their PII.

62. Defendants owed a duty of care not to subject Plaintiff and the Class to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

63. Defendants knew, or should have known, that its security practices and computer systems did not adequately safeguard the PII of Plaintiff and the Class.

64. Defendants breached their duties of care by failing to provide fair, reasonable, or adequate computer systems and security practices to safeguard the PII of Plaintiff and the Class.

65. Defendants breached their duties of care by failing to provide prompt notice of the data breach to the persons whose personal information was compromised.

66. Defendants acted with reckless disregard for the security of the PII of Plaintiff and the Class because Defendants knew or should have known that their computer systems and data security practices were not adequate to safeguard the PII that it collected and stored, which hackers were attempting to access.

67. Defendants acted with reckless disregard for the rights of Plaintiff and the Class by failing to provide prompt and adequate notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use of PII compromised in the Data Breach.

68. Defendants had a special relationship with Plaintiff and the Class. Plaintiff's and the Class' willingness to entrust Defendants with their personal information was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems (and the PII that they stored on them) and to implement security practices to protect the PII that they collected and stored from attack.

69. Defendants own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PII. Defendants' misconduct included failing to:

a. Secure its employees' email accounts;

b. Secure access to its servers;

c. Comply with current industry standard security practices;

d. Encrypt PII during transit and while stored on Defendants' systems;

e. Properly and adequately train their employees on proper data security practices;

f. Implement adequate system and event monitoring;

g. Implement the systems, policies, and procedures necessary to prevent hackers from accessing and utilizing PII transmitted and/or stored by Defendants;

h. Undertake periodic audits of record-keeping processes to evaluate the safeguarding of PII;

i. Develop a written records retention policy that identifies what information must be kept and for how long;

j. Destroy all discarded employee information, including information on prospective employees, temporary workers, subcontractor, and former employees;

k. Secure PII and limit access to PII to those with a legitimate business need;

l. Employ or contract with trained professionals to ensure security of network servers and evaluate the systems used to manage e-mail, Internet use, and so forth;

m. Collect only essential PII from employees, prospective employees, and subcontractors;

n. Avoid using Social Security numbers as a form of identification; and

o. Have a plan ready and in position to act quickly should a theft or data breach occur.

70. Defendants also had independent duties under the laws of the states in which they do business that required them to reasonably safeguard Plaintiff's and the Class' PII and promptly notify them about the Data Breach.

71. Defendants breached the duties they owed to Plaintiff and Class members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols and practices sufficient to protect their PII both before and after learning of the Data Breach;

c. By failing to comply with the minimum industry data security standards before, during, and after the period of the Data Breach; and

d. By failing to timely and accurately disclose that the PII of Plaintiff and the Class had been improperly acquired or accessed in the Data Breach.

72. But for Defendants wrongful and negligent breach of the duties they owed Plaintiff and the Class members, their PII either would not have been compromised or they would have been able to prevent some or all of their damages.

73. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of further harm.

74. The injury and harm that Plaintiff and Class members suffered (as alleged above) was reasonably foreseeable.

75. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendants' negligent conduct.

76. Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II – NEGLIGENCE PER SE
(Brought by the Nationwide Class or, alternatively, 40 Statewide Classes)

77. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

78. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiff and the Nationwide Negligence Per Se Class or, alternative, the Separate Statewide Negligence Per Se Classes (collectively, the "Class" as used in this Count).

79. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as LeafFilter, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also formed part of the basis of Defendants' duty in this regard.

80. Defendants solicited, gathered, and stored PII of Plaintiff and the Class as part of its business of manufacturing, selling, and installing gutter protection systems, which affects commerce.

81. Defendants violated the FTCA by failing to use reasonable measures to protect the PII of Plaintiff and the Class and not complying with applicable industry standards, as described herein.

82. Defendants' violation of the FTCA constitutes negligence *per se*.

83. Plaintiff and the Class are within the class of persons that the FTCA was intended to protect.

84. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC even provides a guide to businesses outlining five key principles for preventing the very harm suffered by Plaintiff and the Class as a result of the Data Breach. *See* "Protecting Personal Information: A Guide for Business" found at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Oct. 26, 2018).

85. According to state laws in the following twelve (12) states in which Defendants do business and/or in which Plaintiff and/or Class members reside, Defendants had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' personal information:

a. **Arkansas**: Ark. Code § 4-110-104;

b. **California**: Cal Civ. Code § 1798.81.5;

c. **Connecticut**: Conn. Gen. Stat. § 42-471;

d. **Florida**: Fla. Stat. § 501.171(2);

e. **Indiana**: Ind. Code § 24-4.9-3.5;

f. **Louisiana**: La. Rev. Stat. § 51:3074(A);

g. **Maryland**: Md. Code. Comm. Law § 14-5303;

h. **Massachusetts**: Mass. Gen Laws Ch. 93H, § 2(a);

i. **North Carolina**: N.C. Gen. Stat. § 75-62;

j. **Oregon**: Ore. Rev. Stat. § 646A.622(1);

k. **Rhode Island**: R.I. Gen Laws § 11-49.2-2(2);

l. **Texas**: Tex. Bus. & Com. Code § 521.052(a); and

m. **Utah**: Utah Code § 14-44-201(1)(a).

86. Defendants uses the same computer systems and security practices in all states in which they operate.

87. Defendants breached their duties to Plaintiff and the Class under these states' laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class' PII.

88. According to state laws in the following forty (40) states in which Defendants do business and/or in which Plaintiff and/or Class members reside, Defendants had a duty to provide notice to Plaintiff and the Class of the Data Breach:

a. **Alabama**: Ala. Code § 8-38-5(a), (b) (notice of a "breach of security" or "breach" shall be made "as expeditiously as possible and without unreasonable delay");

b. **Arkansas**: Ark. Code § 4-110-105(a) (notice of a "breach of the security of the system" shall be made "in the most expedient time and manner possible and without unreasonable delay");

c. **California**: Cal. Civ. Code § 1798.82 (notice of a "breach of the security of the system… shall be made in the most expedient time possible and without unreasonable delay");

d. **Colorado**: Colo. Rev. Stat. § 6-1-716(2) (notice of a "security breach… must be made in the most expedient time possible and without unreasonable delay but not later than thirty days after the date of determination that a security breach occurred");

e. **Connecticut**: Conn. Gen. Stat. § 36a-701b(b)(1) (notice of a "breach of security" shall be made "without unreasonable delay but not later than ninety days after the discovery of such breach");

f. **Delaware**: Del. Code Ann. tit. 6 § 12B-102 (notice of a "breach of security" must be made "without unreasonable delay but not later than 60 days after determination of the breach of security");

g. **Florida**: Fla. Stat. § 501.171(4) (notice of a "breach of security" or "breach" shall be made "as expeditiously as practicable and without unreasonable delay");

h. **Georgia**: Ga. Code § 10-1-912(a) (notice of "any breach of the security of the system" shall be made "in the most expedient time possible and without unreasonable delay");

i. **Illinois**: 815 Ill. Comp. Stat. 530/10 (notice of a "breach of the security of the system data" or "breach" shall be made "in the most expedient time possible and without unreasonable delay");

j. **Indiana**: Ind. Code § 24-4.9-3-3 (notice of a "breach of the security of data" or "breach" shall be made "without unreasonable delay");

k. **Iowa**: Iowa Code § 715C.2 (notice of a "breach of security" shall be made "in the most expeditious manner possible and without unreasonable delay");

l. **Kansas**: Kan. Stat. § 50-7a02 (notice of a "security breach" must be made "in the most expedient time possible and without unreasonable delay");

m. **Kentucky**: Ky. Rev. Stat. § 365.732(2) (notice of a "breach of the security of the system" shall be made "in the most expedient time possible and without unreasonable delay");

n. **Louisiana**: La. Rev. Stat. § 51:3074(E) (notice of "breach in the security of the system" shall be made "in the most expedient time possible and without unreasonable delay");

o. **Maine**: 10 Me. Rev. Stat. § 1348 (notice of a "breach of the security of the system" shall be made "as expediently as possible and without unreasonable delay");

p. **Maryland**: Md. Code, Comm. Law § 14-3504 (notice of a "breach of the security of a system" shall be given "as soon as reasonably practical, but not later than 45 days");

q. **Massachusetts**: Mass. Gen. Laws 93H § 3(a) (notice of a "breach of security" shall be made "as soon as practicable and without unreasonable delay");

r. **Michigan**: Mich. Comp. Laws §§ 445.72(4) (notice of a "breach of the security of a database" or a "security breach" shall be provided "without unreasonable delay");

s. **Minnesota**: Minn. Stat. § 325E.61(a) (notice of any "breach of the security of the system" must be made "in the most expedient time possible and without unreasonable delay");

t. **Mississippi**: Miss. Code § 75-24-29(3) (notice of a "breach of security" shall be made "without unreasonable delay");

u. **Missouri**: Mo. Rev. Stat. § 407.1500(2) (notice of a "breach of security" or "breach" shall be made "without unreasonable delay");

v. **Nebraska**: Neb. Rev. Stat. § 87-803(1) (notice of a "breach of the security of the system" shall be made "as soon as possible and without unreasonable delay");

w. **New Hampshire**: N.H. Rev. Stat. § 359-C:20 (notice of "security breach" shall be made "as soon as possible");

x. **New Jersey**: N.J. Stat. §§ 56:8-163(a) (notice of a "breach of security" shall be made "in the most expedient time possible and without unreasonable delay");

y. **New York**: N.Y. Gen. Bus. Law § 899-aa(2) (notice of a "breach of the security of the system" shall be made "in the most expedient time possible and without unreasonable delay");

z. **North Carolina**: N.C. Gen. Stat. § 75-65(a) (notice of a "security breach" shall be made "without unreasonable delay");

aa. **Ohio**: Ohio Rev. Code §§ 1349.19(B)(2) (notice of any "breach of the security of the system" shall be made in "the most expedient time possible but not later than forty-five days following its discovery");

bb. **Oklahoma**: OKLA. STAT., tit. 24, § 163(A) (notice of any "breach of the security of the system" shall be made "without unreasonable delay");

cc. **Oregon**: Or. Rev. Stat. §§ 646A.604 (notice of a "breach of security" shall be made "as soon as is practicable after discovering a breach of security");

dd. **Pennsylvania**: 73 Pa. Stat. § 2303(a) (notice of any "breach of the security of the system" shall be made "without unreasonable delay");

ee. **Rhode Island**: R.I. Gen. Laws § 11-49.3-4(a)(2) (notice of any "breach of the security of the system" shall be made "in the most expedient time possible, but no later than forty-five (45) calendar days after confirmation of the breach");

ff. **South Carolina**: S.C. Code § 39-1-90(A) (notice of a "breach of the security of the system" must be made "in the most expedient time possible and without unreasonable delay");

gg. **Tennessee**: Tenn. Code Ann. § 47-18-2107(b) (notice of a "breach of system security" shall be made "no later than forty-five days from the discovery or notification of the breach of system security");

hh. **Texas**: Tex. Bus. & Com. Code § 521.053(b) (notice of a "breach of system security" shall be made "as quickly as possible");

ii. **Utah**: Utah Code § 13-44-202(2) (notice of a "breach of system security" shall be made "in the most expedient time possible without unreasonable delay");

jj. **Vermont**: 9 V.S.A. § 2435(b) (notice of a "security breach" shall be made "in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification");

kk. **Virginia**: Va. Code § 18.2-186.6; Va. Code § 32.1-127.1:05; Va. Code § 58.1-341.2

ll. **Washington**: Wash. Rev. Code § 19.255.010(2) (notice of any "breach of the security of the system" shall be made "immediately following discovery");

mm. **West Virginia**: W.V. Code § 46A-2A-102 (notice of any "breach of the security of the system" shall be made "without unreasonable delay"); and

nn. **Wisconsin**: Wis. Stat. § 134.98(2) (notice of a data breach shall be made "within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information").

89. Defendants notified all persons, regardless of which state they reside in, of the Data Breach on or about October 4, 2018.

90. Defendants knew on or before August 21, 2018 that unauthorized persons had accessed and/or viewed or were reasonably likely to have accessed and/or viewed private, protected, personal information of Plaintiff and the Class.

91. Defendants breached their duties to Plaintiff and the Class under the laws of the 40 states in which they do business and/or in which Plaintiff and/or Class members reside by unreasonably delaying and failing to provide notice expeditiously and/or as soon as practicable to Plaintiff and the Class of the Data Breach.

92. Defendants' violation of the FTCA, the state data security statutes listed in paragraph 85, and/or the state data breach notification statutes listed in paragraph 88 constitute negligence *per se*.

93. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach by, *inter alia*, having to spend time reviewing their accounts and credit reports for unauthorized activity; spend time and incur costs to place and re-new a "freeze" on their credit; be inconvenienced by the credit freeze, which requires them to spend extra time unfreezing their account with each credit bureau any time they want to make use of their own credit; and becoming a victim of identity theft, which may cause damage to their credit and ability to obtain insurance, medical care, and jobs.

94. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendants' negligence *per se*.

COUNT III – BREACH OF IMPLIED CONTRACT
(Brought by the Nationwide Class or, alternatively, 40 Statewide Classes)

95. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

96. When Plaintiff and the members of the Nationwide class or, alternatively, the members of the Separate Statewide Breach of Implied Contract Classes (collectively, the "Class" as used in this Count), provided their PII to Defendants when seeking employment or doing business with Defendants, they entered into implied contracts by which Defendants agreed to protect their PII and timely notify them in the event of a data breach.

97. Defendants required its employees, prospective employees, and/or subcontractors, including Plaintiff, to provide PII in order to apply for and/or take a job or do business with Defendants.

98. Defendants implicitly and/or affirmatively represented that they collected and stored the PII of Plaintiff and the members of the Class using reasonable, industry standard means.

99. Based on the implicit understanding and also on Defendants' representations (as described above), Plaintiff and the Class accepted Defendants' offers and provided Defendants with their PII.

100. Plaintiff and Class members would not have provided their PII to Defendants had they known that Defendants would not safeguard their PII as promised or provide timely notice of a data breach.

101. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendants.

102. Defendants breached the implied contracts by failing to safeguard Plaintiff's and Class members' personal information and failing to provide them with timely and accurate notice of the Data Breach.

103. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendants' breach of the implied contract with Plaintiff and Class members.

COUNT IV – INJUNCTIVE / DECLARATORY RELIEF
(Brought by Nationwide Class or, alternatively, 40 Statewide Classes)

104. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

105. Plaintiff and members of the Class entered into an implied contract that required Defendants to provide adequate security for the PII it collected from Plaintiff and the Class.

106. Defendants owe a duty of care to Plaintiff and the members of the Class that requires them to adequately secure PII.

107. Defendants still possess PII regarding Plaintiff and members of the Class.

108. Since the Data Breach, Defendants have announced no changes to their data security infrastructure, processes or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Data Breach to occur and go undetected for months and, thereby, prevent further attacks.

109. Defendants have not satisfied their contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendants' lax approach towards information security is known to hackers, the PII in Defendants possession is even ***more*** vulnerable to cyber attack.

110. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiff and the members

of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their PII and Defendants' failure to address the security failings that lead to such exposure.

111. There is no reason to believe that Defendants' security measures are any more adequate now than they were before the breach to meet Defendants' contractual obligations and legal duties.

112. Plaintiff, therefore, seeks a declaration (1) that Defendants' existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendants' segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants cease transmitting PII via email;

f. Ordering that Defendants cease storing PII in email accounts;

g. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

h. Ordering that Defendants conduct regular database scanning and securing checks;

i. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendants to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendants as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, punitive damages, attorney's fees, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendants to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

Dated: November 2, 2018

Respectfully Submitted,

/s/ *William B. Federman*

William B. Federman, TBA #00794935
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Avenue
Oklahoma City, OK 73120
-and-
2926 Maple Ave., Ste. 200
Dallas, TX 75201
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com

ATTORNEY FOR PLAINTIFF AND
THE PROPOSED CLASS